



PUBLIC SECTOR

## Federal Agencies – Will Sarbanes-Oxley Fit?

### A Discussion of Federal Internal Controls

AUDIT

AUDIT ■ TAX ■ ADVISORY

© 2004 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International.

## Introduction

**Members of Congress and representatives of federal government agencies have begun discussions that could eventually lead to the requirement for federal agency management to provide an assertion in their agency's financial statements on their internal controls over financial reporting and to obtain an independent auditor's opinion on those internal controls. In effect, the federal government is inching toward applying the same type of reporting requirements to federal agencies that are now required of publicly traded companies under section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley).**

Under Sarbanes-Oxley section 404, management of public companies is required to:

- Accept responsibility for the effectiveness of the entity's internal control over financial reporting
- Evaluate the effectiveness of the entity's internal control over financial reporting using suitable control criteria, for example, those defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Support the evaluation with sufficient evidence, including documentation
- Present a written assessment about the effectiveness of the company's internal control over financial reporting as of the end of the entity's most recent fiscal year



If such a requirement were adopted by federal agencies, it would mark a major shift in current procedures and policies. It could strengthen the confidence of the American taxpayers in the government, improve the effective use of federal resources, and provide more accountability.

With that scenario as a backdrop, this document aims to provide ideas on understanding and preparing for the internal control reporting requirements that federal agency management might soon face.

## Background

### A Federal Call to Action

For the past seven years, the federal government has been unable to issue an opinion to the Congress and U.S. taxpayers on whether the government's financial statements are fairly stated in conformity with U.S. generally accepted accounting principles (GAAP).<sup>1</sup> Although many federal agencies have made strides in correcting deficiencies in their financial statement reporting, David M. Walker, Comptroller General of the United States, said earlier this year that the federal government has a long way to go before it can issue such an opinion.

In a February 27, 2004, statement to Congress, Comptroller General Walker said that until "a significant number of material weaknesses related to financial systems, fundamental record keeping and financial reporting, and incomplete documentation" are addressed, the weaknesses "will continue to (1) hamper the federal government's ability to accurately report a significant portion of its assets, liabilities, and costs; (2) affect the federal government's ability to accurately measure the full cost as well as the financial and non-financial performance of certain programs while effectively managing related operations; and (3) significantly impair the federal government's ability to adequately safeguard significant assets and properly record various transactions."<sup>2</sup>

### BACKGROUND OF SARBANES-OXLEY

The credibility of public company financial reporting has been sharply questioned by a string of corporate reporting scandals that began with the collapse of a number of major corporations in late 2001. The results shook the financial markets and severely eroded investor confidence in the information being reported by companies with publicly traded securities.

These historic events led to a number of proposals to improve the financial reporting process and restore investor confidence in the U.S. financial markets. Congress responded with the passage of the Sarbanes-Oxley Act. When President George W. Bush signed the Act into law, he characterized it as "the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt."

The Act clearly represents the most significant change in reporting for U.S. publicly traded companies since the Securities Acts of 1933 and 1934. It is aimed at restoring public confidence and protecting the public interest as well as improving the integrity of financial reporting—the foundation on which the U.S. capital markets system is built and thrives.

The passage of this Act represents a significant change in both management's reporting responsibilities and the scope and nature of the responsibilities of the independent auditor. Management is now required to both assess and report on the effectiveness of internal control over financial reporting, and the auditor is required to audit and report on the effectiveness of internal control over financial reporting, including management's assessment. As a result, auditors will be evaluating and testing a company's internal control in a different light and in greater depth. The overall goal of these new requirements is to strengthen internal control over financial reporting, provide more reliable information to investors, and renew investor confidence in the U.S. capital markets.

<sup>1</sup> Letter to President George W. Bush and Congress from U.S. Comptroller General, David M. Walker, February 27, 2004.

<sup>2</sup> Ibid.

In the realm of publicly traded companies, the SEC rules implementing section 404(a) of Sarbanes-Oxley focus on those objectives related to the reliability of a company's external financial reporting.

As these reporting circumstances persist, questions arise about whether it is inconsistent for the Congress to require publicly traded companies to follow one set of regulations (Sarbanes-Oxley section 404) for internal control reporting while not requiring federal agencies to follow those same regulations. "Government should lead by example," Walker said in a June 2003 *CFO Magazine* article. "We should be as good or better than those we are regulating."<sup>3</sup>

#### **DEFINITION OF INTERNAL CONTROL OVER FINANCIAL REPORTING**

Internal control is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance of the achievement of objectives in the following categories: effectiveness and efficiency of operations, compliance with applicable laws and regulations, and reliability of financial reporting.

In the realm of publicly traded companies, the SEC rules implementing section 404(a) of Sarbanes-Oxley focus on those objectives related to the reliability of a company's external financial reporting. This subset of internal control is commonly referred to as internal control over financial reporting. Internal control over financial reporting is defined in the Public Company Accounting Oversight Board's (PCAOB) Standard No. 2 as a process designed by or under the supervision of the company's principal executive and financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP). It also includes policies and procedures that pertain to maintenance of accounting records, authorization of receipts and disbursements, and safeguarding of assets.

For purposes of an audit of internal control over financial reporting, "internal control over financial reporting" includes controls over the safeguarding of assets and controls related to the prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets that could have a material effect on the financial statements. These safeguarding controls are a subset of the broader segment of internal control.

<sup>3</sup> "Feds Fail Again," *CFO Magazine*, June 2003.

A bill currently before the House (H.R. 4259) contains a provision for a study of the potential costs and benefits of requiring all 23 Chief Financial Officers Act (CFO Act) agencies to obtain audit opinions on internal control over their financial reporting. The same bill, if passed, would require that the Secretary of the Department of Homeland Security include in its Performance and Accountability Report for fiscal year 2005 an assertion on the internal controls that apply to that department's financial reports. Further, the bill would require the Department of Homeland Security's internal controls to be the subject of an annual audit opinion by an independent auditor. A member of the management team at a CFO Act agency said in recent discussions that a cost-benefit analysis of requiring an audit opinion of internal control over financial reporting is crucial: "From my perspective, you've got to balance between making sure that you are having a substantial review, and not just spending dollars chasing dimes."

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires the heads of the 23 CFO Act agencies to annually evaluate and report on the agency's systems of internal accounting and administrative control. FMFIA directs the Office of Management and Budget (OMB) to establish guidelines for the evaluation by agencies of their systems of internal accounting and administrative control. Those guidelines are set forth in OMB Circular A-123, *Management Accountability and Control*, which define internal control using 10 components. This compares to 27 internal control components contained in the COSO guidance, which is the internal control framework used most often by public companies that are subject to section 404 of Sarbanes-Oxley.

"From my perspective, you've got to balance between making sure that you are having a substantial review, and not just spending dollars chasing dimes."

Member, CFO Act agency





## The Significance of a Strong Federal Control Framework

Since it is not a requirement for federal agencies to have an auditor's opinion on internal control over financial reporting, most do not currently obtain such an opinion. Several agencies voluntarily obtained an auditor's opinion on internal control over financial reporting in fiscal years 2002 or 2003. An early 2004 review of these opinions, however, shows inconsistency in the control frameworks used by the agencies to evaluate their internal controls and in the control frameworks referenced by the auditors in their related opinions. A review by KPMG of the financial reports of the 23 CFO Act agencies showed that three received an auditor's opinion on internal control over financial reporting in fiscal year 2003. Eight other agencies, not subject to the CFO Act, received an opinion on internal control over financial reporting in fiscal years 2002 and 2003.

### THE FIVE COSO COMPONENTS OF INTERNAL CONTROL OVER FINANCIAL REPORTING

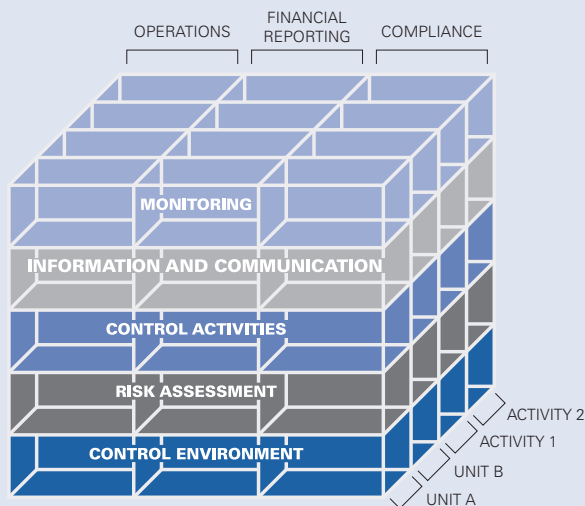
**Control Environment** – The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

**Risk Assessment** – Every entity faces a variety of financial reporting risks from external and internal sources that must be assessed both at the entity and the activity level. These risks include external and internal events and circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial data consistent with the assertions of management embodied in the financial statements.

**Control Activities** – Control activities are the policies and procedures that help ensure management directives are carried out. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed.

**Information and Communication** – Pertinent information must be identified, captured, and communicated in a form and timeframe that supports all other control components. The quality of system-generated information, including the accounting system and other information technology applications, affects management's ability to make appropriate decisions in controlling the entity's activities and to prepare reliable financial reports.

**Monitoring** – Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time.



Source: KPMG LLP in the U.S., 2004.

Of those eleven opinions,<sup>4</sup> three contained management's assertion on the effectiveness of internal control—a requirement under Sarbanes-Oxley section 404. As a criteria for evaluating internal control over financial reporting:

- Two of the eleven opinions referenced the General Accounting Office's (GAO) *Standards for Internal Control in the Federal Government* (the Green Book)
- Three referenced FMFIA
- Two referenced auditing guidance contained in OMB Bulletin 01-02 (*OMB's Guidance on Performing Audits of Federal Agencies*)
- Three referenced both FMFIA and OMB Bulletin 01-02
- One referenced a management directive, similar to FMFIA

The variety of frameworks used as references by the agencies underscores the need for the use of a consistent set of criteria, such as is the case with the use of COSO by publicly traded companies that are following the regulations of Sarbanes-Oxley section 404. A consistent set of criteria could lead to increased comparability and also could make the audits of internal control more comprehensive.

A consistent control framework is critical because it determines the extent to which management reviews, documents, and tests internal control over financial reporting. The following chart compares the COSO internal control components with those components contained in the frameworks used by the eleven federal agencies reviewed by

KPMG. When comparing the internal control framework criteria used by those agencies, the extent of coverage is significantly less under OMB Circular A-123 and Bulletin 01-02 than the internal control coverage provided under the COSO framework criteria.

Independent audit firms must follow auditing and attestation standards in order to issue an opinion on internal control over financial reporting. These standards define a complete and allowable internal control framework. In practice, it appears that most federal agencies are using internal control frameworks that are a subset of a complete framework.

Another defining element of an allowable framework is that the proposed criteria must have been made available for public comment. Some of the criteria now being used by federal agency management for internal control reporting have not been made available for public comment.

COSO and the GAO's Green Book include a number of elements that are not included in OMB Circular A-123 and Bulletin 01-02, specifically in the areas of risk assessment, information and communication, and monitoring. If federal agency management does not test in those significant areas, its assertion would not be as comprehensive regarding the effectiveness of internal control over financial reporting as an assertion that is required under Sarbanes-Oxley section 404.



<sup>4</sup> GSA ('03), NRC ('03), SSA ('03), U.S. Customs ('02), ATF ('02), GPO ('03), PBGC ('03), FDIC ('03), BPD ('03), IRS ('03), and GAO ('03).

## COMPARISON OF INTERNAL CONTROL FRAMEWORKS

Components of a Complete Internal Control Framework <sup>5</sup>	COSO	GAO's Green Book	OMB A-123	OMB 01-02
<b>Control Environment</b>				
Integrity and Ethical Values	✓	✓	✓	
Commitment to Competence	✓	✓	✓	
Management's Relationship with its Oversight Agency (e.g., Board of Directors, Audit Committee, Congress, OMB)	✓	✓		
Management's Philosophy and Operating Style	✓	✓	✓	
Organizational Structure	✓	✓	✓	
Assignment of Authority and Responsibility	✓	✓	✓	
Human Resource Policies and Practices	✓	✓	✓	
<b>Risk Assessment</b>				
Entity-Wide Objectives	✓	✓		
Activity-Level Objectives	✓	✓		
Risk Identification	✓	✓		
Risk Analysis	✓	✓		
Managing Change	✓	✓		
<b>Control Activities</b>				
Policies and Procedures	✓	✓		
Top-Level Reviews	✓	✓	✓	✓
Direct Functional or Activity Management	✓	✓	✓	
Information Processing	✓	✓	✓	✓
Physical Controls	✓	✓	✓	✓
Performance Indicators	✓	✓		
Segregation of Duties	✓	✓	✓	
<b>Information and Communication</b>				
Strategic and Integrated Systems	✓	✓	✓	
Information Quality	✓	✓	✓	
Internal Communication	✓	✓	✓	
External Communication	✓	✓		
Means of Communication	✓	✓		
<b>Monitoring</b>				
Ongoing Monitoring Activities	✓	✓		
Separate Evaluations	✓	✓		
Reporting Deficiencies	✓	✓	✓	✓

Source: KPMG LLP in the U.S., 2004.

<sup>5</sup> The COSO report's definition of internal control, including the five components, was incorporated by amendment in 1995 into Statement on Auditing Standards (SAS) No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, Professional Standards, Vol. 1, AU Sec. 319), as amended.



## Benefits of Improved Internal Control Over Financial Reporting by Federal Agencies

With more effective controls, there can be a strengthening in the confidence of the American people in government, an improvement in the effectiveness of federal programs, and more accountability.



The job of improving internal control over financial reporting within federal agencies—as well as subjecting management’s internal control assertion to independent audit—will take considerable time and will be difficult. But without effective controls, “fraud, waste, and abuse in federal activities and programs lead to the loss of billions of dollars of government funds, erode public confidence, and undermine the federal government’s ability to operate effectively.”<sup>6</sup> With more effective controls, there can be a strengthening in the confidence of the American people in government, an improvement in the effectiveness of federal programs, and more accountability.

Though the job ahead will be difficult, McCoy Williams, Director, GAO Financial Management and Assurance, said in recent testimony before a House subcommittee, “implementation of a strong system of internal control will likely not be easy or quick and will require strong support and continuous action from the President, the Congress, top-level administration appointees, and agency management officials. Once committed to a plan of action, they must remain steadfast supporters of the

end goals and their support must be transparent to all. Agencies must be held accountable for appropriately managing and controlling their programs and safeguarding program assets. OMB must continue to provide direction and support to agency management in the implementation of government-wide efforts, such as those involving improper payments, and conduct appropriate oversight of federal agency efforts to meet their stewardship and program management responsibilities.”<sup>7</sup>

In some respects, the current debate on how to improve federal agency internal control reporting is similar to the debate in the late 1980s that preceded the eventual passage of the 1990 CFO Act. Until its passage, federal agencies were not required to have independently audited financial statements. Several years passed after the Act was put in place before the statements were auditable. In hindsight,

prudent managers of federal agencies would have prepared much sooner to be able to produce financial statements that could receive a clean (unqualified) audit opinion. Similarly, there are parallels now for financial officers at federal agencies preparing for potential OMB or GAO directives requiring an internal control assessment and an audit opinion on internal control over financial reporting. In conclusion, a consistent framework that meets the applicable standard should be specified for use by management and auditors to assess and report on internal controls over financial reporting.

<sup>6</sup> McCoy Williams, Director, GAO Financial Management and Assurance, April 15, 2004, in testimony before the Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform, House of Representatives

<sup>7</sup> Ibid.

## Examples of Public Companies Deriving Value From the Sarbanes-Oxley Process

**Executives at several businesses that had made substantial progress with their Sarbanes-Oxley initiatives shared their views with KPMG. Before the Sarbanes-Oxley effort, for example, a multibillion-dollar utility needed nearly 200 people and 22 days to complete its closing process. The manual nature of the process typically resulted in unexpected results as well as entries of significance after the company released earnings. The Sarbanes-Oxley compliance review process prompted the company to examine the extent of its manual processes for the first time. The company is now reengineering the closing process so that it will require half as many people and just 10 days to complete.**

In another case, a financial services organization discovered that many of its derivatives traders used vastly different methods to place a value on its derivatives. The concern about the possibility of inconsistencies led to a standardization of pricing methods that has reassured the financial services organization's CFO about the accuracy of asset values on the organization's balance sheet.

In documenting their internal control over financial reporting, organizations are amassing large amounts of detailed information about their business processes, risks, and controls.

In documenting their internal control over financial reporting, organizations are amassing large amounts of detailed information about their business processes, risks, and controls. In so doing, some of them have come to realize that risk tolerances are inconsistent across divisions. Others have discovered insufficient understanding of the risk-assessment process at many levels within the enterprise. They are using their compliance efforts as a foundation to:

- Strengthen, streamline, and automate internal controls
- Increase an enterprise-wide understanding of all risks—operational, financial reporting, and compliance—and how to control them
- Improve and redesign business processes while maintaining appropriate awareness and control of risks



Thus, these companies have moved beyond the immediate short-range project state into a long-range sustainable life cycle that helps capture value and offers continuous performance improvement. Armed with access to an extraordinary range of information about their processes, risks, and controls, they can begin to evaluate potential process improvements as well as whether they have the right controls and are controlling the right things.

## Applying Internal Control Reporting to Federal Agencies



Management should undertake a self-assessment process to understand how the agency can document, assess, and refine its internal controls over financial reporting.

**An important step now facing federal agency management is the recognition that it is never too early to plan for change. Management should undertake a self-assessment process to understand how the agency can document, assess, and refine its internal controls over financial reporting.**

The process that management undertakes in its assessment should include identifying its controls, determining the locations or units to include in the evaluation (if the agency has multiple locations or units), determining which controls management should test, and evaluating the likelihood that failure of a control could result in a material financial statement or disclosure misstatement.

Management should also evaluate the design and operating effectiveness of internal control over financial reporting and document the results of the evaluation. This process ordinarily would be considered incomplete unless it is extended to controls over all relevant assertions related to all significant accounts and disclosures.

As part of its assessment, management determines if identified deficiencies in design or operating effectiveness—individually or in combination—constitute reportable conditions (referred to now as “significant deficiencies” under Sarbanes-Oxley) or material weaknesses. Management then communicates these findings to the auditor and others, if applicable, and evaluates whether those findings are reasonable and support its assessment.

### Documentation Supporting Management’s Assessment

Documentation that provides reasonable support for management’s assessment of the effectiveness of internal control over financial reporting includes, but is not limited to:

- The design of controls over relevant assertions related to all significant accounts and disclosures in the financial statements, including documentation of the five components of the COSO framework
- Information about how significant transactions are initiated, authorized, recorded, processed, and reported
- Information about the flow of transactions to identify where material misstatements due to error or fraud could occur
- Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties
- Controls over the period-end financial reporting process
- Controls over safeguarding of assets
- The results of management’s testing and assessment

### Significant Effort

One of the most pressing questions about the Sarbanes-Oxley section 404 requirements is “How much will it cost to comply?” Since there is little historical data to answer this question, surveys can provide some useful information.

In January 2004, Financial Executives International (FEI) conducted a survey of 321 public companies and found that the companies expected to spend an average of 12,265 hours internally to comply with section 404 requirements dealing with management reporting on internal controls. The FEI report also found that the number of hours “is directly proportional to the size of the company. For example, companies with less than \$25 million in revenues expected to spend an average of 1,150 hours, while companies with over \$5 billion in revenues expected to spend an average of 35,000 hours.”<sup>8</sup>

In a separate survey performed in late 2003 by KPMG, 39 companies reported that they expected external auditors to begin their attestation engagement an average of 7.4 months ahead of year-end. Nearly three quarters (72 percent) expected external auditors to begin their attestation engagement at least six months prior to their fiscal year-end.

One third of the companies in the KPMG study identified 250 significant controls or fewer, another third identified between 250 and 500 significant controls, and most of the others identified between 500 and 1,000 controls.

The FEI survey found that companies expected to pay an average of \$732,100 for external consulting, software, and other vendor charges to comply with section 404, excluding auditor’s fees for attestation. Companies with less than \$25 million in revenues expected to pay an average of \$170,000, while companies with over \$5 billion in revenues expected to pay an average of \$1,390,100. The costs for these types of services at certain federal agencies could well exceed these amounts.

The attest effort for internal control over financial reporting could approximate or even exceed the effort expended in the financial statement audit. However, the final determination of incremental fees is highly dependent on the facts and circumstances of each situation.

Although this survey information is helpful, amounts of time and costs may vary significantly from these survey amounts. Factors that will affect these variances include: size and complexity of the entity, number of locations and processing sites, extent and quality of controls that are already documented, and the mix of internal and external resources available.

Regardless of the lack of historical information on the level of effort required, one can confidently conclude that *the costs and efforts will be significant*.

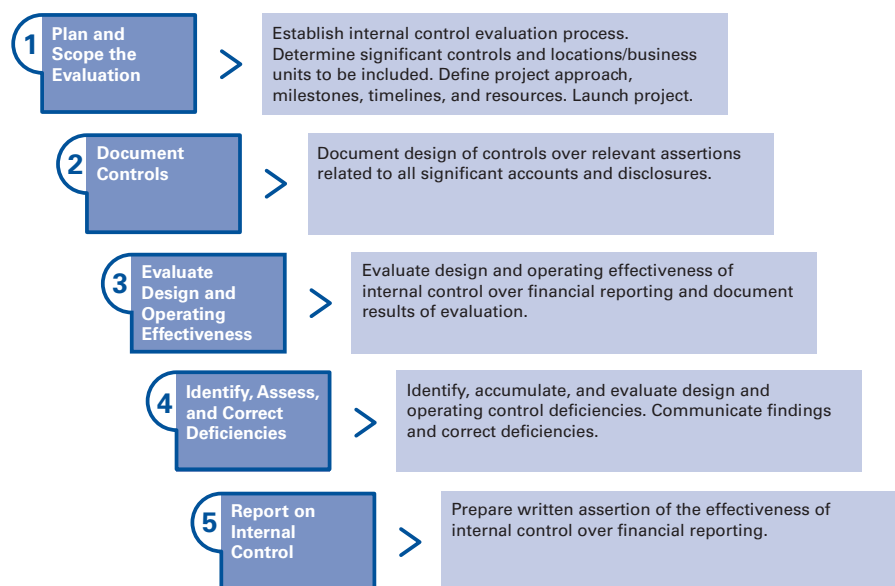
Regardless of the lack of historical information on the level of effort required, one can confidently conclude that the costs and efforts will be significant.

<sup>8</sup> FEI Survey on Sarbanes-Oxley Section 404 Implementation/January 2004. Copyright FEI, 2004.

## Example Assessment Process for Federal Agencies



There are a number of methods an agency could use in developing an approach to assessing its internal control over financial reporting. The following is one example of how a public company may approach its assessment process, which we believe can be applied to federal agencies.



Source: KPMG LLP in the U.S., 2004.

**1 Plan and Scope the Evaluation**

The process of evaluating the effectiveness of internal control over financial reporting may require careful planning due to the complexity and breadth of the control structure within an entity. This evaluation plan may include a process to examine the overall approach to documentation, identification of controls and evaluation procedures, significant milestones, and anticipated timelines. The plan also may include the institution of policies and procedures that will be used in the evaluation process, as well as appropriate internal communication processes.

Management may identify the team responsible for performing the evaluation. The project may have an executive sponsor, a project manager, and personnel from operations, budget, finance and accounting, human resources, information systems, and legal—all of whom should have appropriate skills, knowledge of COSO and the *GAO Standards for Internal Control in the Federal Government* (Green Book), and an understanding of controls evaluation. Where necessary, management may consider training programs to supplement their existing knowledge.



Among the most important activities in the planning process is one that identifies the controls that are to be included in the scope of the evaluation.

Among the most important activities in the planning process is one that identifies the controls that are to be included in the scope of the evaluation. The evaluation should include controls related to all significant accounts and disclosures in the financial statements.

#### EVALUATION OF IT CONTROLS

Information technology (IT) controls represent an integral part of internal control over financial reporting. Management may determine which applications or systems are within the scope of internal control over financial reporting and which IT controls need to be evaluated (i.e., user-level and infrastructure). An evaluation of an agency's IT controls also may determine whether existing systems have been changed or a new system has been put in place. Controls within the system are important, but so are the controls dealing with access to IT systems. Management would be well-served by evaluating details of the following broad categories of the IT function:

##### IT general controls:

- Program development
- Program and system changes
- Access to programs and data
- Computer operations

##### Application/process controls:

- Authorization
- Configuration/account mapping
- Exception/edit reports
- Interface/conversion
- System access

The specific risks that IT poses to an entity's internal control may include the reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both. IT also may involve the risk of unauthorized access to systems, including unauthorized changes to existing applications, as well as unauthorized changes to data, and the potential for loss of data.

A financial statement caption may consist of a number of account balances, the components of which are subject to differing risks or different controls that should be considered separately as potential significant accounts. These significant accounts are subject to different financial reporting risks and different controls.

#### 2 Document Controls

Documentation of an entity's internal control over financial reporting is an essential part of management's evaluation process. It provides evidence that controls related to management's assertion—including changes to those controls—have been identified, are capable of being communicated to those responsible for their performance, and are capable of being monitored.

Documentation of controls may take many forms and can include a variety of information, including policy manuals, process models, flowcharts, job descriptions, documents, and forms. The extent of documentation may vary, depending on the size, nature, and complexity of the entity. Management should consider establishing entity-wide documentation standards for capturing and reporting information. Documentation of processes and controls will be an important element in the test of internal control design effectiveness.

Although the extent to which management documents its evaluation is a matter of judgment, such documentation should go beyond a simple conclusion that the control is designed and operating effectively. To provide a sufficient basis for its conclusion, management should document the procedures performed, the results, and other evidence obtained regarding operating effectiveness. Internal control deficiencies noted also should be documented along with appropriate remediation proposals. Inadequate documentation of the design of controls and the absence of sufficient documented evidence to support management's assessment of the operating effectiveness of internal control over financial reporting could be considered control deficiencies.

COSO provides example documentation that could be useful for management in documenting the results of its evaluation. The examples in COSO include numerous evaluation programs and worksheets.

To collate and evaluate the documentation of the results of the evaluation, management may consider either a manual or an automated approach, or a combination of the two. Either way, management may consider establishing enterprise-wide documentation standards for capturing the results. An automated tool may assist in ensuring that the documentation output of the evaluation process meets management's requirements. With the use of an automated tool, the information could be summarized and reported in a format tailored by management. An added benefit of using an automated tool may be to assist with project management, for example, to monitor the progress of the documentation and evaluation process and identify areas that need attention.

### 3 Evaluate Design and Operating Effectiveness

Management will need to evaluate the design and operating effectiveness of internal control over financial reporting, and it should document the results of this evaluation.

#### Design

Effectively designed controls are expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements. All controls necessary to provide reasonable assurance regarding the fairness of an entity's financial statements should be in place and performed and monitored by qualified personnel.

#### DESIGN AND OPERATING EFFECTIVENESS

*Design effectiveness* refers to whether a control is suitably designed to prevent or detect material misstatements in specific financial statement assertions. It involves consideration of the financial reporting objectives that the control is meant to achieve.

*Operating effectiveness* refers to whether the control is functioning as designed. During the evaluation of operating effectiveness, management gathers evidence regarding how the control was applied, the consistency with which it was applied, and who applied it.

Management must evaluate the design of relevant controls. Procedures to evaluate design effectiveness could include inquiry, observation, and a specific evaluation of whether the controls are likely to prevent or detect misstatements if they are operated as prescribed by appropriately qualified persons.

#### Operating Effectiveness

In evaluating whether a control is operating effectively, an entity may consider whether the control is operating as designed and whether the person performing the control possesses the necessary authority and qualifications to perform the control effectively.

Management must perform procedures sufficient to assess the operating effectiveness of controls. These procedures could include testing of the controls by internal audit, testing of the controls by others under the direction of management, using a service organization's reports, or testing by means of a self-assessment process. Inquiry alone will not be adequate to complete this evaluation by management.

**4 Identify, Assess, and Correct Deficiencies**

Management may establish a process by which deficiencies are identified

and accumulated across the entire entity, including all locations evaluated. To conclude on the assessment of effectiveness of internal control over financial reporting, management is likely to evaluate the severity of all identified deficiencies.

*An internal control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. An internal control deficiency may be either a design or operating deficiency.*

A design deficiency exists when either a necessary control is missing or an existing control is not properly designed so that even when the control is operating as designed, the control objective is not always met. An operating deficiency exists when a properly designed control either is not operating as designed or the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

A deficiency is significant if it results in more than a remote likelihood that a misstatement that is more than inconsequential in amount will not be prevented or detected. This definition establishes a relatively low threshold in making the significance determination.

Internal control deficiencies range from inconsequential internal control deficiencies to material weaknesses in internal control. Management should determine whether the internal control deficiency is inconsequential, significant, or represents a material weakness. Personnel throughout the entity should share a common understanding of these definitions and how they are applied. Federal agencies may find it useful to understand how the PCAOB has defined a significant deficiency and a material weakness:

*A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects a company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP such that there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.*

*A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.*

If there are significant deficiencies that, individually or in combination, result in one or more material weaknesses, management is precluded from concluding that internal control over financial reporting is effective.

As defined by the PCAOB, a misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement is considered more than inconsequential.

The PCAOB also identifies certain areas that, if deficiencies exist, are deemed to be at least significant deficiencies. These areas include:

- Controls over the selection and application of accounting policies in accordance with GAAP
- Antifraud programs and controls
- Controls over non-routine and non-systematic transactions
- Controls over the period-end financial reporting process

The PCAOB identifies a number of circumstances that, because of their likely significant negative effect on internal control over financial reporting, are significant deficiencies and *strong indicators* that a material weakness exists. These circumstances include:

- Restatement of previously issued financial statements to reflect the correction of a misstatement, whether due to error or fraud
- Identification by the auditor of a material misstatement in financial statements in the current period that was not initially identified by the entity (even if management subsequently corrects the misstatement)
- For larger, more complex entities, ineffective risk-assessment functions
- Identification of fraud of any magnitude on the part of senior management
- Significant deficiencies that have been communicated to management that remain uncorrected after some reasonable period of time
- An ineffective control environment

Management should allow sufficient time to evaluate and test controls. In the event deficiencies are discovered, management will have the opportunity to correct and remediate these deficiencies prior to the reporting date. However, management will need to allow enough time for new controls to be in place to validate their operating effectiveness.

## 5 Report on Internal Control

Federal agencies may want to consider how publicly traded companies are expected to issue a management report on internal control over financial reporting. The report is required to include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the entity
- A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the entity's internal control over financial reporting
- An assessment of the effectiveness of the entity's internal control over financial reporting as of the end of its most recent fiscal year, including an explicit statement as to whether that internal control over financial reporting is effective
- A statement that the public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the entity's internal control over financial reporting and an assessment on the entity's internal control over financial reporting

Management is required to provide a written conclusion about the effectiveness of the entity's internal control over financial reporting. This conclusion can take many forms; however, management is required to state a direct conclusion about its effectiveness. Other phrases, such as "management's

assessment that the entity's internal control over financial reporting as of [date] is sufficient to meet the stated objectives," also might be used. However, the conclusion should not be so subjective (for example, "very effective internal control") that people having competence in and using the same or similar criteria would not ordinarily be able to arrive at similar conclusions.



## Key Points to Remember



Leading the assessment from the executive level helps ensure that the project priority is properly set, that resources are made available, and that findings are properly addressed.

**Entities that have been performing management assessments of internal control over financial reporting find certain actions key to successfully realizing operational benefits from improving the control structure. Actions include:**

- Leading the assessment from the executive level makes it likely that the project priority is properly set, that resources are made available, and that findings are properly addressed. This level of leadership fosters an environment that when issues are identified, they are addressed and resolved in a timely manner, since the assessment process is, in itself, a control process that must be carried out in the course of one fiscal year.
- Involving the Office of the Inspector General early in the process to help ensure that the management assessment process and the eventual audit of management's assessment and internal controls are well integrated, avoid redundant efforts, and work together to maximize operational benefits.
- Performing the project in accordance with the GAO's Green Book to promote all elements, including risk assessment, general control environment, and general IT control environment are assessed, documented, appropriately tested, and reported upon.
- Encouraging a clear chain of command for the project so that project deadlines are adhered to, management has adequate time to consider and address any control gaps that are identified, and remediation plans are executed prior to year-end to allow for additional testing. A remediation action performed at year-end leaves little time for the required testing to ensure the control is properly functioning at year-end. Without performing the required testing, management does not have the evidence to support the assertion that the control is functioning.

Managing the project is crucial to the success of the effort in that objectives must be clearly defined, process documentation must be collected and evaluated, documentation must be improved in some cases, and the controls identified for testing must be documented. During the project management process, the planning, testing, and reporting phases must be kept on track so that benefits are realized. The output will be the documentation of testing results—including the remediation of any control gaps—which will form the basis for management's assertion. Therefore, timeliness is critical.



# KPMG LLP

KPMG LLP is the audit, tax, and advisory firm that has maintained a continuous commitment throughout its history to providing leadership, integrity, and quality. The Big Four firm with the strongest growth record over the past decade, KPMG turns knowledge into value for the benefit of its clients, people, communities, and the capital markets. Its professionals work together to provide clients access to global support, industry insights, and a multidisciplinary range of services. KPMG LLP ([www.us.kpmg.com](http://www.us.kpmg.com)) is the U.S. member firm of KPMG International. KPMG International's member firms have nearly 100,000 professionals, including 6,800 partners, in 148 countries.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Visit KPMG on the World Wide Web at [www.us.kpmg.com](http://www.us.kpmg.com).

© 2004 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A. The KPMG logo and name are trademarks of KPMG International. 26788atl

# Contacts

For further information on internal control over financial reporting by federal government agencies, please contact any of the following KPMG professionals:

Terry Carnahan, 703-286-8334  
[tcarnahan@kpmg.com](mailto:tcarnahan@kpmg.com)

John Cherbini, 202-533-4339  
[jcherbini@kpmg.com](mailto:jcherbini@kpmg.com)

Diane Dudley, 202-533-3002  
[ddudley@kpmg.com](mailto:ddudley@kpmg.com)

Terry Henzey, 703-286-8400  
[thenzey@kpmg.com](mailto:thenzey@kpmg.com)

John Hummel, 202-533-3008  
[jhummel@kpmg.com](mailto:jhummel@kpmg.com)

Dan Kovlak, 202-533-6072  
[dkovlak@kpmg.com](mailto:dkovlak@kpmg.com)

Andrew C. Lewis, 202-533-4886  
[aclewis@kpmg.com](mailto:aclewis@kpmg.com)

Ron Longo, 202-533-4014  
[rlongo@kpmg.com](mailto:rlongo@kpmg.com)

Scott Showalter, 201-505-5500  
[dsshowalter@kpmg.com](mailto:dsshowalter@kpmg.com)

